First Hit Fwd Refs

□ Generate Collection Print

L2: Entry 4 of 10 File: USPT Jun 26, 2001

DOCUMENT-IDENTIFIER: US 6252869 B1
TITLE: Data network security system and method

Abstract Text (1):
A secure communication mechanism for communicating credit card or other sensitive information between a user terminal and a server which communicate over a data network (e.g.,Internet). For secure or private communication of sensitive information over a data network, a telephone connection is established between the originating server to which the user is connected for access to the data network and the SP to which the sensitive information is directed. The method and system provide for a secure electronic commercial transaction between a user and a service provider which charges for information and/or services and/or goods, wherein sensitive information includes credit card information transmitted from the user to the service provider, and/or electronic information or services transmitted from the service provider to the user in exchange for payment received from the user.

Brief Summary Text (4):
Currently, a multitude of services are available to users over data networks such as the Internet. These services include information and interactive services deliverable over the network, and goods and services that may be shopped for and ordered over the network but are not deliverable over the network (e.g., clothing, food, etc.). Despite the plethora of available services and the apparent convenience for consumers of virtual shopping from electronic merchants or service providers (SPs), individuals are generally wary of electronic shopping and particularly, are reluctant to send credit card or other sensitive information over the Internet, since it is well publicized that personal credit card information should not be transmitted over a public data network, which may be subject to unauthorized access. It is also well publicized that individuals have cracked security coding mechanisms (e.g., RSA encryption) used in commercial software for secure communications on the Internet. It is therefore possible, for instance, that while en route to a targeted SP, encrypted credit card or other sensitive information may be intercepted at intervening routers by "hackers" or other eavesdroppers, who can decrypt the information.

Brief Summary Text (6):
It may be understood that the lack of a secure transaction mechanism limits the further development of the Internet, the availability of service providers to users, and particularly the viability of smaller SPs. It is known that in addition to providing gateway access to the Internet and the thousands of small service providers around the world, large information service providers such as Prodigy, America Online and Compuserve provide their own information and interactive services. Users may also access the Internet and the thousands of smaller information service providers (ISPs) directly through smaller user-local Internet access providers. Generally, the large information service providers bill their customers on a time-usage basis after a financial payment relationship has been established, with the user/customer receiving a monthly bill which may include additional charges for usage of certain information and services and which is paid via the conventional postage system. Similarly, the smaller user-local Internet access providers usually also base their service charges to their subscribers for access to the Internet on a time-usage basis.

Brief Summary Text (7):
The smaller ISPs, however, currently either do not charge for access to their information and interactive services, or, if they do, also require the user to establish some sort of financial relationship whereby the user subscribes to the ISP and pays a bill via the conventional postage system. A frequent user of a particular established ISP may not be adverse to establishing a financial relationship for payment purposes. Typically, however, and in accordance with a fundamental concept of using the Internet (e.g., "surfing the net" using Web browsers which link websites by hypertext), a user accesses many different ISPs, each on only a casual and often unanticipated basis, and is not likely to want or be able to establish a plethora of financial relationships with so many different providers. ISPs that do or want to charge for access to their information and/or interactive services could do so by requiring the user to input their credit card number before data service is provided. Yet, as discussed above, users are loath to sending credit card information over the Internet, and therefore, would likely eschew such ISPs, who are typically smaller ISPs.

Brief Summary Text (8):
Accordingly, it may be appreciated that from the standpoint of the user/consumer, such a security and privacy risk effectively preempts the ostensible convenience of services available over data networks, and also limits the actual availability of information and interactive services to those which are free of charge or are charged within the purview of existing financial relationships (e.g., information from a user's service provider). From the standpoint of the SPs, the absence of a secure on-line billing mechanism limits the virtual marketplace, and its potential returns. In addition, the lack of a secure payment mechanism limits the number of SPs which can enter this marketplace, thereby limiting competition which would also likely benefit users/consumers.

Brief Summary Text (14):
In another embodiment, the user may selectively invoke secure communications (e.g. by clicking on an icon on the user's terminal screen) to communicate to the user's originating access SP server (or, to the terminating ISP server) that a secure communication link over the telephone line should be established with the terminating ISP server (originating access SP server) for communicating sensitive information from the user to the terminating ISP. The originating access SP server (the terminating ISP) then verifies that the terminating ISP server (originating access SP server) supports the secure communication mechanism. Upon verification, a telephone connection is established between the originating access SP server and the terminating ISP server, and the sensitive information is communicated. The telephone connection is terminated in accordance with user commands or the transmitted information itself. In a further related embodiment, when a transaction of sensitive information is to occur but the user does not choose to invoke a secure telephone connection for sending credit card information but relies on conventional mechanisms, the terminating ISP server can initiate establishment of a secure telephone communication link with the originating access SP server in order to send electronic goods/services to the user.

Brief Summary Text (15):
In a similar embodiment, the user's originating access SP server initiates establishment of a secure telephone communication link with the terminating ISP server upon identifying a communication from the user that includes sensitive or private information.

Detailed Description Text (2):
With reference to FIG. 1, a system is shown which provides access for users on a data network to information and/or interactive services, and for a secure communication mechanism on a telephone network for the provision of those services. For purposes of illustration and clarity of exposition, it will be assumed that the

data network is the Internet, and that the secure communication involves providing user credit card information to a service provider (SP) as payment for providing information and/or interactive services, including electronically deliverable and/or non-electronically deliverable goods and services. It is understood, however, that the present invention is not limited to secure payment communications, or to payment for information and/or interactive services only on the Internet.

Detailed Description Text (8):
In accordance with the present invention, communication of credit card or other sensitive information (including electronically deliverable goods/services) between a user and an ISP on the Internet (or other data network) is effected by a separate telephone call connection (i.e., over the public switched telephone network) established between the user's Internet access provider and the ISP. The establishment of the telephone connection is initiated in response to actions of the user. For instance, the user may explicitly request a secure communication link or the user may request a page from the ISP that involves credit card or sensitive information. Alternatively, the user may send credit card or other payment information to the ISP to purchase electronically-deliverable goods/services from the ISP but may choose to forego an option of requesting a secure communication link for sending the credit card or payment information to the ISP; nevertheless, in response to this payment, the terminating ISP may choose to complete the transaction (i.e., by sending the electronically-deliverable good/services to the user) over a secure communication link. The Internet's access provider or the terminating ISP may first recognize that the user's actions require establishing the separate telephone connection. In any event, the telephone connection may be established according to the user's originating Internet access SP calling the terminating ISP, resulting in the telephone connection charges being incurred by the originating Internet access SP and passed along to the user according to the normal established billing arrangement. Alternatively, the telephone connection may be established according to the terminating SP calling the originating SP, resulting in the telephone connection charges being incurred by the terminating SP (unless charges are "reversed" by, for example, using a special access number), who may account for such costs in charges to users. After the telephone connection is established, it is used for communicating the sensitive information, after which the telephone connection is terminated.

Detailed Description Text (12):
Alternatively, web pages provided by ISP 101 may include a DNS icon such that when the user invokes (i.e., clicks on) the icon, the ISP 101 is sent a message which explicitly requests that the current web page on terminal 104 be sent by the DNS (i.e., that the web page be considered a secure page). Similarly, although the user may have an option for invoking DNS in order to purchase electronically-deliverable goods/services, the user may send credit card or payment information to ISP 101 by a conventional mechanism (e.g., over the Internet). From the user's actions of paying for electronically-deliverable goods/services, ISP 101 recognizes that a secure communication link should be established to complete the transaction by delivering the electronically-deliverable goods/services in a manner that protects their value to ISP 101.

Detailed Description Text (13):
Based on these explicit and/or implicit requests according to the user's actions and associated conditions, ISP 101 recognizes that a secure communication link must be established for the secure page and thus, initiates a protocol for establishing a telephone connection by querying Internet access provider 107 via Internet 102 as to whether Internet access provider 107 supports DNS (step 403).

Detailed Description Text (22):
It may be appreciated, therefore, that the present invention provides many features, advantages, and attendant advantages for users and service providers on

data networks. From the user's standpoint, a secure payment method is available which frees use for previously offerred but inadvisable transactions, thereby effectively providing the user with not only convenience but also with information, services, and goods previously not easily located or available external to the Internet. From the ISP's standpoint, a method of receiving payment is provided which facilitates increasing the market and demand for the supplied information and/or interactive services, and/or non-electronic goods or services. In addition, the secure communication method should result in increased use and development of the Internet, as well as reduced cost to the user.

CLAIMS:

10. The method according to claim 1, wherein said first two-way communications link aims to form a point-to-point connection between said orioinating server and said terminating server.

11. The method according to claim 1, wherein said step of establishing the separate connection includes the steps of:

said terminating server providing a telephone number to said originating server over the first two-way communications link;

said originating server placing a call using said telephone number; and

said terminating server receiving said call and thereby establishing said separate connection.

13. The method according to claim 1, wherein said step of establishing the separate connection includes the steps of:

said originating server providing a telephone number to said terminating server over the first communications link on the data network;

said terminating server placing a call using said telephone number; and

said originating server receiving said call.

15. A method for communicating information between a user and a terminating server, said user connected to said terminating server via an accessing server which is connected to said terminating server over a data network by a first communications link, said method comprising the steps of:

at the terminating server:

associating a telephone call with said user;

establishing, in coordination with said accessing server, a telephone connection with said accessing server;

communicating said information with said accessing server via said telephone connection while said first communication link connection continues to be active;

at the accessing server:

establishing, in coordination with said terminating server, said telephone connection;

associating said telephone connection with said user;

communicating said information with said terminating server via said telephone connection; and

communicating said information with said user.

16. The method according to claim 15, wherein said step of establishing a telephone connection includes the steps of:

said terminating server providing a telephone number to said accessing server over the first communications link on the data network;

said accessing server placing a call using said telephone number; and

said terminating server receiving said call.

18. The method according to claim 15, wherein said step of establishing the separate connection includes the steps of:

said accessing server providing a telephone number to said terminating server over the first communications link on the data network;

said terminating server placing a call using said telephone number; and

said accessing server receiving said call.

20. A system for secure communication, comprising:

an originating server;

a terminating server connected to said originating server over a packet data network by a first two-way communications link that includes at least one switching or routing active node and which carries information from said originating server to said terminating server and from said terminating server to said originating server;

a dialer for establishing a secure connection between said originating server and said terminating server that is distinct from the first two-way communications link; and

means for transmitting at least some of said information via the secure connection while said first two-way communications link is active.

25. A method for communicating first sensitive information possessed by a first party to a second party, and communicating second sensitive information possessed by the second party to the first party, where said first party is connected to said second party via a first two-way communication link of a data network, where information that is not sensitive flowing from said first party to said second party, and vice versa over said first two-way communication link of said data network by means of data packets, said method comprising the steps of:

transmitting a phone number from said first party to said second party over said first two-way link;

placing a call over a telecommunications network that is distinct from said data network, using said phone number, from said second party to said first party;

receiving said call at said first party to provide a secure telephone connection over said telecommunications network between the first party and the second party; and

transmitting said first sensitive information and said second sensitive information over said secure telephone connection.

28. A method for communicating sensitive information from a first internet service provider (ISP) server to a second ISP server, where the first ISP server and the second ISP server are connected to each other by means of a primary connection over a packet network, said method comprising the steps of:

While maintaining said primary connection, establishing a connection between said first ISP server and said second ISP server that is more secure than said primary connection; and

transmitting said sensitive information via the more secure connection while said primary connection is active.